The US-CERT Cyber Security Bulletin provides a summary of new and updated vulnerabilities, exploits, trends, and malicious code that have recently been openly reported. Information in the Cyber Security Bulletin is a compilation of open source and US-CERT vulnerability information. As such, the Cyber Security Bulletin includes information published by sources outside of US-CERT and *should **not** be considered the result of US-CERT analysis or as an official report of US-CERT*. Although this information does reflect open source reports, it is not an official description and should be used for informational purposes only. The intention of the Cyber Security Bulletin is to serve as a comprehensive directory of pertinent vulnerability reports, providing brief summaries and additional sources for further investigation.

Vulnerabilities

The tables below summarize vulnerabilities that have been reported by various open source organizations or presented in newsgroups and on web sites. **Items in bold designate updates that have been made to past entries.** Entries are grouped by the operating system on which the reported software operates, and vulnerabilities which affect both Windows and Unix/ Linux Operating Systems are included in the Multiple Operating Systems table. *Note*, entries in each table are not necessarily vulnerabilities *in* that operating system, but vulnerabilities in software which operate on some version of that operating system.

Entries may contain additional US-CERT sponsored information, including Common Vulnerabilities and Exposures (CVE) numbers, National Vulnerability Database (NVD) links, Common Vulnerability Scoring System (CVSS) values, Open Vulnerability and Assessment Language (OVAL) definitions, or links to US-CERT Vulnerability Notes. Metrics, values, and information included in the Cyber Security Bulletin which has been provided by other US-CERT sponsored programs, is prepared, managed, and contributed by those respective programs. CVSS values are managed and provided by the US-CERT/ NIST National Vulnerability Database. Links are also provided to patches and workarounds that have been provided by the product's vendor.

The Risk levels are defined below:

High - Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

Medium - Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.

Low - Vulnerabilities will be labeled "Low" severity if they have a CVSS base score of 0.0-3.9.

Note that scores provided prior to 11/9/2005 are approximated from only partially available CVSS metric data. Such scores are marked as "Approximated" within NVD. In particular, the following CVSS metrics are only partially available for these vulnerabilities and NVD assumes certain values based on an approximation algorithm: AccessComplexity, Authentication, ConfImpact of 'partial', IntegImpact of 'partial', AvailImpact of 'partial', and the impact biases.

Windows Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources

AspSitem 1.83	An input validation vulnerability has been reported in AspSitem that could let remote malicious users perform SQL injection. AspSitem 2.0 There is no exploit code required.	AspSitem SQL Injection	Not Available	SecurityFocus, ID: 17616, April 19, 2006
McAfee VirusScan 10.0.21, SecurityCenter Agent 6.0.0.16	A buffer overflow vulnerability has been reported in VirusScan, DUNZIP32.dll, that could let remote malicious users obtain unauthorized access. Upgrade to newest version of DUNZIP32.dll via tools online update capabilities. **Updated to correct erroneous CVE information.** There is no exploit code required.	McAfee VirusScan Unauthorized Access **CVE-2004-1094**	10	Secunia, Advisory: SA19460, March 30, 2006
Microsoft Internet Explorer	Multiple vulnerabilities have been reported in Internet Explorer that could let remote malicious users execute arbitrary code. Microsoft **A Proof of Concept exploit has been published.**	Microsoft Internet Explorer Arbitrary Code Execution CVE-2006-1185 CVE-2006-1186 CVE-2006-1188 CVE-2006-1189 CVE-2006-1190 CVE-2006-1191 CVE-2006-1192 CVE-2006-1245 CVE-2006-1359 CVE-2006-1388	7.0 (CVE-2006-1185) 10 (CVE-2006-1186) 7.0 (CVE-2006-1188) 10 (CVE-2006-1189) 10 (CVE-2006-1190) 3.7 (CVE-2006-1191) 1.9 (CVE-2006-1192) 7.0 (CVE-2006-1245) 7.0 (CVE-2006-1359) 7.0 (CVE-2006-1388)	Microsoft, Security Bulletin MS06-013, April 11, 2006 US-CERT VU#434641, VU#503124, VU#341028, VU#824324, VU#959649, VU#984473, VU#959049, VU#876678 National Cyber Alert System SA06-101A Technical Cyber Security Alert TA06-101A
Neon Software Neon Responders 5.4	A vulnerability has been reported in Neon Responders that could let remote malicious users cause a denial of service. No workaround or patch available at time of publishing. A Proof of Concept exploit script, neon_responder_dos.c, has been published.	Neon Responders Denial of Service	Not Available	SecurityFocus, ID: 17569, April 10, 2006
ShixxNOTE 6.net	A buffer overflow vulnerability has been reported in ShixxNOTE 6.net that could let remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ShixxNOTE 6.net Arbitrary Code Execution	Not Available	SecurityFocus, ID: 11409, April 17, 2006

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources

ALWIL Software Avast! Linux Home Edition 1.0.5	A vulnerability has been reported due to insecure permissions on a folder in the '/tmp' directory when performing a virus scan, which could let a remote malicious user create, overwrite, or manipulate arbitrary file permissions. No workaround or patch available at time of publishing. There is no exploit code required.	Avast! Linux Home Edition Insecure Temporary File Creation	Not Available	Secunia Advisory: SA19683, April 18, 2006
Asterisk Asterisk 1.2.6, 1.2 .0-beta2, 1.2 .0-beta1, 1.0.7-1.0.9, 0.9 .0, 0.7.0- 0.7.2, 0.2-0.4, 0.1.7-0.1.9 -1	An integer overflow vulnerability has been reported when handling a malformed JPEG file, which could let a remote malicious user execute arbitrary code. Patches available Currently we are not aware of any exploits for this vulnerability.	Asterisk JPEG File Integer Overflow CVE-2006-1827	4.7	Security Focus, Bugtraq ID: 17561, April 17, 2006
BannerFarm BannerFarm 2.3	A Cross-Site Scripting vulnerability has been reported in 'banners.cgi' due to insufficient sanitization of the 'aff' and 'cat' parameters, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	BannerFarm Cross-Site Scripting	Not Available	Secunia Advisory: SA19718, April 19, 2006
Censtore Censtore 7.3.002 & prior	A vulnerability has been reported in 'censtore.cgi' due to insufficient sanitization of the 'page' parameter before using, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit script, vi censtore-RCE.pl, has been published.	Censtore Remote Arbitrary Command Execution CVE-2006-1799	7.0	Security Focus, Bugtraq ID: 17515, April 13, 2006
Horde Project Horde Application Framework 3.0.9 & prior	A vulnerability has been reported in 'services/go.php' due to insufficient verification of the 'url' parameter before using in a 'readfile()' call, which could let a remote malicious user obtain sensitive information. Updates available Gentoo **dsa-1033** **dsa-1034** Currently we are not aware of any exploits for this vulnerability.	Horde Information Disclosure CVE-2006-1260	2.3	Secunia Advisory: SA19246, March 15, 2006 Gentoo Linux Security Advisory, GLSA 200604-02, April 4, 2006 **Debian Security Advisories, DSA-1033-1 & DSA-1034, April 12 & 14, 2006**
Horde Project Horde Application Framework 3.0-3.0.7	HTML injection vulnerabilities have been reported due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available **dsa-1033** There is no exploit code required.	Horde Application Framework HTML Injection CVE-2005-4190	1.4	Secunia Advisory: SA17970, December 12, 2005 **Debian Security Advisory, DSA-1033-1, April 12, 2006**
IBM AIX 5.3 L, 5.3, 5.2 L, 5.2, 5.1 L, 5.1	A vulnerability has been reported in the 'rm_mlcache_file' command due to an unspecified error, which could let a malicious user obtain elevated privileges. Fixes available Currently we are not aware of any	IBM AIX Elevated Privileges CVE-2006-1247	3.3	Security Tracker Alert ID: 1015952, April 18, 2006

	exploits for this vulnerability.			
Multiple Vendors Debian Linux 3.1 sparc Debian Linux 3.1 s/390 Debian Linux 3.1 ppc Debian Linux 3.1 mipsel Debian Linux 3.1 mips Debian Linux 3.1 m68k Debian Linux 3.1 ia-64 Debian Linux 3.1 ia-32 Debian Linux 3.1 hppa Debian Linux 3.1 arm Debian Linux 3.1, amd64, alpha, 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; bsd-games bsd-games 2.12-2.14, 2.9, 2.17	Multiple buffer overflow vulnerabilities have been reported due to insufficient bounds-checking when copying user-supplied input to insufficiently sized memory buffers, which could let a malicious user obtain elevated privileges. **dsa-1036** Currently we are not aware of any exploits for these vulnerabilities.	BSD-Games Buffer Overflows CVE-2006-1744	4.9	Security Focus, Bugtraq ID: 17401, April 7, 2006 **Debian Security Advisory, DSA-1036-1, April 17, 2006**
Multiple Vendors FCheck 2.7.59; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	A vulnerability has been reported due to the insecure creation of temporary files, which could let a malicious user obtain sensitive information. Debian There is no exploit code required.	FCheck Insecure Temporary File Creation CVE-2006-1753	3.3	Security Focus, Bugtraq ID: 17524, April 15, 2006 Debian Security Advisory, DSA-1035-1, April 15, 2006
Multiple Vendors Linux Kernel 2.6.x	A vulnerability has been reported because AMD K7/K8 CPUs only save/restore certain x87 registers in FXSAVE instructions when an exception is pending, which could let a remote malicious user obtain sensitive information. Updates available FreeBSD Currently we are not aware of any exploits for this vulnerability.	Linux Kernel x87 Register Information Leak CVE-2006-1056	Not Available	Secunia Advisory: SA19724, April 19, 2006 FreeBSD Security Advisory, FreeBSD-SA-06:14, April 19, 2006
Multiple Vendors Linux kernel 2.6-2.6.16	A Denial of Service vulnerability has been reported when program control is returned using SYSRET on Intel EM64T CPUs. Updates available Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Intel EM64T SYSRET Denial of Service CVE-2006-0744	1.6	Secunia Advisory: SA19639, April 17, 2006
Multiple Vendors Linux kernel 2.6-2.6.16	A Denial of Service vulnerability has been reported in 'perfmon.c' on ia64 platforms during exit processing. A patch is available to address this issue. An exploit has been published.	Linux Kernel 'Perfmon.c' Denial of Service CVE-2006-0558	2.3	Security Focus, April 12, 2006
Multiple Vendors Linux kernel 2.6-2.6.16, 2.5-2.5.69, 2.4-2.4.33	A vulnerability has been reported regarding shared memory access, which could let a malicious user bypass security restrictions. Patches available Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Shared Memory Security Restriction Bypass CVE-2006-1524	Not Available	Security Focus, Bugtraq ID: 17587, April 18, 2006

Multiple Vendors Linux Kernel prior to 2.6.16.8	A Denial of Service vulnerability has been reported in the 'ip_route_input()' function when requesting a multi-cast IP address. Updates available Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IP_ROUTE_INPUT Denial of Service CVE-2006-1525	Not Available	Secunia Advisory: SA19709, April 19, 2006
NetBSD NetBSD 3.0, 2.1, 2.0-2.0.3, 1.6- 1.6.2	A vulnerability has been reported because the driver for Intel's RNG (Random Number Generator) incorrectly detects the device as present on some hardware, which could lead to weakened security features. Updates available Currently we are not aware of any exploits for this vulnerability.	NetBSD Intel RNG Driver Detection CVE-2006-1833	Not Available	Security Tracker Alert ID: 1015907, April 13, 2006
NetBSD NetBSD 3.0, 2.1, 2.0-2.0.3, 1.6- 1.6.2	A Denial of Service vulnerability has been reported due to an exceptional condition arising when the SIOCGIFALIAS IOCTL is used to get information about an alias of an interface. Updates available Currently we are not aware of any exploits for this vulnerability.	NetBSD SIOCGIFALIAS IOCTL Denial of Service CVE-2006-1797	2.3	Security Tracker Alert ID: 1015908, April 13, 2006
NetBSD NetBSD 3.0, 2.1, 2.0-2.0.3, 1.6- 1.6.2	A Denial of Service vulnerability has been reported in 'sysctl()' calls because the size of a user-supplied buffer isn't checked against system resource limits. Updates available Currently we are not aware of any exploits for this vulnerability.	NetBSD 'sysctl()' Denial of Service CVE-2006-1814	1.6	Security Tracker Alert ID: 1015909, April 13, 2006
PHP Net Tools PHP Net Tools 2.7.1	A vulnerability has been reported in 'nettools.php' due to insufficient sanitization of the 'host' parameter before using when executing a shell command, which could let a remote malicious user execute arbitrary commands. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, an exploit script, PHPNetTools-rce.pl, has been published.	PHP Net Tools Shell Command Execution	Not Available	Secunia Advisory: SA19694, April 19, 2006
Smarter Scripts IntelliLink Pro 5.06	Cross-Site Scripting vulnerabilities have been reported in 'addlink_lwp.cgi' due to insufficient sanitization of the 'url' parameter and in 'edit.cgi' due to insufficient sanitization of the 'id,' 'forgotid,' and 'forgotpass' parameters, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, Proof of Concept exploit scripts have been published.	IntelliLink Pro Multiple Cross-Site Scripting	Not Available	Security Focus, Bugtraq ID: 17605, April 19, 2006
Sun Microsystems, Inc. Java Studio Enterprise 8	A vulnerability has been reported because certain files are installed with world-writable permissions when installed by the 'root' user, which could let a malicious user obtain elevated privileges. Patches available There is no exploit code required.	Sun Java Studio Elevated Privileges CVE-2006-1830	Not Available	Sun(sm) Alert Notification Sun Alert ID: 102292, April 13, 2006

Sybase Sybase Enterprise Application Server 5.2, 5.3	A vulnerability has been reported due to the insecure storage of user credentials in the connection cache, which could let a remote malicious user obtain sensitive information. Workaround & Patch information There is no exploit code required.	Sybase EAServer Manager Information Disclosure CVE-2006-1829	Not Available	Security Tracker Alert ID: 1015913, April 13, 2006
Symantec Norton Utilities for Macintosh 8.0, Norton System Works for Macintosh 3.0, Norton Personal Firewall for Macintosh 3.1, 3.0, Norton Internet Security for Macintosh 3.0, Norton Antivirus for Macintosh 10.9.1, 10.0.1, 10.0 .0, 9.0.3, 9.0.2, 9.0.1, 9.0.0, LiveUpdate for Macintosh 3.5, 3.0.3, 3.0.2, 3.0.1, 3.0, Symantec AntiVirus for Macintosh 10.0	A vulnerability has been reported because the execution path environment for certain components is not set, which could let a malicious user execute arbitrary programs with System Administrative privileges. Apply latest LiveUpdate patch. There is no exploit code required.	Symantec LiveUpdate for Macintosh Elevated Privileges CVE-2006-1836	Not Available	Symantec Security Advisory, SYM06-007, April 17, 2006
Visale Visale 1.0	Cross-Site Scripting vulnerabilities have been reported in 'pbpgst.cgi' due to insufficient sanitization of the 'keyval" parameter, in 'pblscg.cgi' due to insufficient sanitization of the 'catsubno' parameter, and in 'pblsmb.cgi' due to insufficient sanitization of the 'listno' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, Proof of Concept exploit scripts have been published.	Visale Multiple Cross-Site Scripting	Not Available	Security Focus, Bugtraq ID: 17598, April 19, 2006
W3C Amaya 9.4	Several buffer overflow vulnerabilities have been reported when parsing various attribute values due to boundary errors, which could let a remote malicious user execute arbitrary code. Update to version 9.5. Proofs of Concept exploits have been published.	Amaya Buffer Overflows	Not Available	Secunia Advisory: SA19670, April 14, 2006
xFlow xFlow 5.46.11	Multiple vulnerabilities have been reported: an SQL injection vulnerability was reported in 'members_only/index.cgi' due to insufficient sanitization of the 'position' and 'id' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported in 'members_only/index.cgi' due to insufficient sanitization of the 'level,' 'position,' 'id,' and 'action' parameters and in 'customer_area/index.cgi' due to insufficient sanitization of the 'page' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, Proof of Concept	xFlow Multiple Vulnerabilities CVE-2006-1849 CVE-2006-1850 CVE-2006-1851	Not Available	Secunia Advisory: SA19707, April 19, 2006

	exploit scripts have been published.			
xine xine 1.0.1, 1.0, 0.9.18, 0.9.13, 0.9.8, 1-rc8 1-rc0-1-rc7, 1-beta1-beta12	A format string vulnerability has been reported in the 'print_formatted()' function in 'xitk/main.c' when processing a specially crafted playlist, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Xine Playlist Handling Remote Format String	Not Available	Security Focus, Bugtraq ID: 17579, April 18, 2006

[back to top]

Multiple Operating Systems - Windows/UNIX/Linux/Other

Vendor & Software Name	Description	Common Name	CVSS	Resources
AB Webservices RateIt 2.2	An SQL injection vulnerability has been reported in 'Rateit.PHP' due to insufficient sanitization of the 'rateit_id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability be exploited through a web client.	RateIt SQL Injection CVE-2006-1798	7.0	Secunia Advisory: SA19637, April 14, 2006
ActualScripts ActualAnalyzer Server 8.23, ActualAnalyzer Lite 2.72, ActualAnalyzer Gold 7.63	A file include vulnerability has been reported in 'Direct.PHP' due to insufficient verification of the 'rf' parameter, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	ActualScripts ActualAnalyzer Remote File Include	Not Available	Security Focus, Bugtraq ID: 17597, April 19, 2006
Adobe Systems, Incorporated Document Server 5.x, 6.x, Document Server for Reader Extensions 6.x, Adobe Graphics Server 2.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to missing access control restrictions, which could let a remote malicious user obtain authentication credentials; a vulnerability was reported in the 'ReaderURL' parameter in the 'Update Download Site' section due to insufficient sanitization, which could let a remote malicious user execute arbitrary code; a Cross-Site Scripting vulnerability was reported in 'ads-readerext' due to insufficient sanitization of the 'actionID' parameter and in 'Adobe Server Web Services' (AlterCast) due to insufficient sanitization of the 'op' parameter, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported in 'ads-readerest' because a different error message is returned when attempting to log on depending on the validity of the username, which could let a remote malicious user obtain sensitive information; and a vulnerability was reported in 'ads-readerext' because a user's session ID is exposed, which could let a remote malicious user obtain sensitive information. Updates available Vulnerabilities may be exploited with a web browser; however, Proof of Concept exploits have been published.	Adobe Document Server for Reader Extensions Vulnerabilities CVE-2006-1627 CVE-2006-1785 CVE-2006-1786 CVE-2006-1787 CVE-2006-1788	7.0 (CVE-2006-1627) 1.1 (CVE-2006-1785) 1.9 (CVE-2006-1786) 1.9 (CVE-2006-1787) 1.9 (CVE-2006-1788)	Adobe Security Advisory, April 11, 2006
Adobe Systems, Incorporated LiveCycle Workflow 7.01, LiveCycle Form Manager 7.01	A vulnerability has been reported because a user that has been marked 'OBSOLETE' can still access LiveCycle data, which could let a remote malicious user bypass security restrictions. Workaround & Patch Information There is no exploit code required.	Adobe LiveCycle OBSOLETE User Access Validation CVE-2006-1628	3.4	Adobe Security Advisory, April 11, 2006

ADOdb ADOdb 4.70, 4.68, 4.66	An SQL injection vulnerability has been reported due to insufficient sanitization of certain parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Updates available Gentoo dsa-1029 dsa-1030 dsa-1031 **Gentoo** There is no exploit code required.	ADOdb PostgreSQL SQL Injection CVE-2006-0410	2.3	Secunia Advisory: SA18575, January 24, 2006 Gentoo Linux Security Advisory, GLSA 200602-02, February 6, 2006 Debian Security Advisory, DSA-1029, April 8, 2006 Debian Security Advisory, DSA-1030-1, April 8, 2006 Debian Security Advisory, DSA-1031-1, April 8, 2006 **Gentoo Linux Security Advisory, GLSA 200604-07, April 14, 2006**
ADOdb ADOdb 4.71 & prior	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'adodb_pager.inc.php' due to insufficient sanitization of the 'next_page' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability was reported in 'adodb_pager.inc.php' due to the unsafe use of 'PHP_SELF,' which could let a remote malicious user execute arbitrary HTML and script code. dsa-1029 dsa-1030 dsa-1031 **Gentoo** There is no exploit code required.	ADOdb Multiple Cross-Site Scripting CVE-2006-0806	2.3	Secunia Advisory: SA18928, February 20, 2006 Debian Security Advisory, DSA-1029, April 8, 2006 Debian Security Advisory, DSA-1030-1, April 8, 2006 Debian Security Advisory, DSA-1031-1, April 8, 2006 **Gentoo Linux Security Advisory, GLSA 200604-07, April 14, 2006**
Apache Software Foundation libapreq2 2.0.6	A remote Denial of Service vulnerability has been reported due to errors in the 'apreq_parse_ headers()' and 'apreq_parse_ urlencoded()' functions. Update available Debian DSA 1000-2 **Gentoo** Currently we are not aware of any exploits for this vulnerability.	Apache Libapreq2 Remote Denial of Service CVE-2006-0042	2.3	Security Focus, Bugtraq ID: 16710, February 17, 2006 Debian Security Advisory, DSA-1000-1, March 14, 2006 Debian Security Advisory, DSA 1000-2, April 3, 2006 **Gentoo Linux Security Advisory, GLSA 200604-08, April 17, 2006**
ar-blog ar-blog 5.2	A Cross-Site Scripting vulnerability has been reported in 'print.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	AR-Blog Cross-Site Scripting	Not Available	Security Focus, Bugtraq ID: 17522, April 14, 2006
AWStats AWStats 6.5	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'awstats.pl' due to insufficient sanitization of the 'config' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a path disclosure vulnerability was reported when an invalid 'config' parameter is submitted.	AWStats Cross-Site Scripting & Path Disclosure	Not Available	Secunia Advisory: SA19725, April 19, 2006

	No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.			
BetaBoard BetaBoard 0.1	A HTML injection vulnerability has been reported in 'editprofile.php' due to insufficient sanitization of the 'FormVal_profile' parameter before using, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	BetaBoard HTML Injection	Not Available	Secunia Advisory: SA19700, April 18, 2006
BlackOrpheus BlackOrpheus 1.0	An SQL injection vulnerability has been reported in 'Member.PHP' due to insufficient of the 'userID' parameter before using it in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, an exploit script, Blackorpheus_poc, has been published.	BlackOrpheus SQL Injection	Not Available	Security Focus, Bugtraq ID: 17558, April 16, 2006
Blursoft Blur6ex 0.3.452	A file include vulnerability has been reported in 'index.php' which could let a remote malicious unauthorized user view files and execute local scripts. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	Blursoft Blur6ex File Include CVE-2006-1762	7.0	Security Focus, Bugtraq ID: 17554, April 17, 2006
BN Soft BoastMachine 3.0 platinum	A Cross-Site Scripting vulnerability has been reported in 'search.php' due to insufficient sanitization of the 'key' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	BoastMachine Cross-Site Scripting CVE-2006-1841	Not Available	Security Focus, Bugtraq ID: 17550, April 17, 2006
Calendarix Calendarix Advanced 1.5.20050501, 0.6.20050830	A Cross-Site Scripting vulnerability has been reported in 'yearcal.php' due to insufficient sanitization of the 'ycyear' parameter before returning to users, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	Calendarix Cross-Site Scripting CVE-2006-1835	Not Available	Secunia Advisory: SA19710, April 18, 2006
Chipmunk PHP Scripts Chipmunk Guestbook 1.3	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'username' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	Chipmunk Guestbook SQL Injection CVE-2006-1683	7.0	Secunia Advisory: SA19584, April 13, 2006
Circle R Monster Top List 1.4	A file include vulnerability has been reported in 'Functions.PHP' due to insufficient sanitization of the 'root_path' parameter, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	Monster Top List Remote File Include CVE-2006-1781	7.0	Security Focus, Bugtraq ID: 17546, April 17, 2006
Cisco Systems IOS XR for PRP 3.2.3, IOS XR for CRS-1 3.2.3, XR 3.2.50, XR 3.2.4, 3.2.2, 3.2.1, 3.2	A remote Denial of Service vulnerability has been reported when switching certain MPLS packets. Updates available Currently we are not aware of any exploits for this vulnerability.	Cisco IOS XR MPLS Denial of Service	Not Available	Cisco Security Advisory, cisco-sa-20060419, April 19, 2006
Cisco Systems Wireless Lan Solution Engine, Express 0, 1130 2.0.5, 1130 2.0 .2, 1130 2.0 , 1105 2.5, 1105 2.0.2, 1105	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'ArchiveApplyDisplay.jsp' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported which could let a remote malicious user obtain elevated privileges.	Cisco Wireless Lan Solution Engine Cross-Site Scripting & Privilege Elevation	Not Available	Cisco Security Advisory, cisco-sa-20060419, April 19, 2006

2.0	Workaround & Update information Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.			
Clanscripte.net Fuju News 1.0	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'archiv2.php' due to insufficient sanitization of the 'ID' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported due to an error in the authentication process, which could let a remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, an exploit script, fuju_news.php, has been published.	Fuju News SQL Injection & Authentication Bypass CVE-2006-1837 CVE-2006-1838	Not Available	Security Focus, Bugtraq ID: 17572, April 17, 2006
Cute PHP Team CuteNews 1.4.1	A Cross-Site Scripting vulnerability has been reported in the 'Editnews' module due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	CutePHP CuteNews Cross-Site Scripting	Not Available	Security Focus, Bugtraq ID: 17592, April 19, 2006
dbbs.sup.fr DbbS 2.0-alpha, 2.0	Multiple input validation vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML, script code and SQL code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, Proof of Concept exploits have been published.	DbbS Multiple Input Validation	Not Available	Security Focus, Bugtraq ID: 17559, April 17, 2006
Dubelu PhpGuestbook 1.0	An HTML injection vulnerability has been reported in 'phpguestbook.php' due to insufficient sanitization of the 'Name,' 'Website,' and 'Comment' field parameters, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	Dubelu PHPGuestbook HTML Injection	Not Available	Security Focus, Bugtraq ID: 17594, April 19, 2006
Empire Empire Server 4.3, 4.2	Multiple unspecified security vulnerabilities have been reported. The cause and impact of these issues are currently unknown. Update to version 4.3.1. Currently we are not aware of any exploits for these vulnerabilities.	Empire Server Multiple Unspecified Vulnerabilities CVE-2006-1840	Not Available	Secunia Advisory: SA19674, April 18, 2006
FarsiNews FarsiNews 2.5.3, 2.5, 2.1 Beta2, 2.1	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'search.php' due to insufficient sanitization of the 'selected_search_arch' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a path disclosure vulnerability was reported in the 'archive' parameter value when displaying an error message. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	FarsiNews Cross-Site Scripting & Path Disclosure CVE-2006-1822 CVE-2006-1823	4.7 (CVE-2006-1822) 4.7 (CVE-2006-1823)	Security Tracker Alert ID: 1015943, April 15, 2006
FlexBB FlexBB 0.5.5	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; an exploit script, flexbb.pl, has been published.	FlexBB SQL Injection CVE-2006-1811	4.7	Security Focus, Bugtraq ID: 17568, April 17, 2006

FlexBB FlexBB 0.5.7 & prior	Multiple HTML injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input before using in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client.	FlexBB Multiple HTML Injection CVE-2006-1810	1.6	Security Focus, Bugtraq ID: 17539, April 15, 2006
Gregory DEMAR Coppermine Photo Gallery 1.4.4	A file include vulnerability has been reported in 'Index.PHP' due to insufficient verification of the 'file' parameter, which could let a remote malicious user view and execute arbitrary scripts. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	Coppermine File Include	Not Available	Security Focus, Bugtraq ID: 17570, April 17, 2006
Horde Horde 3.0-3.0.9, 3.1	A vulnerability has been reported in Help Viewer which could let a remote malicious user execute arbitrary PHP code. Updates available SuSE Gentoo **dsa-1033** **dsa-1034** Vulnerability can be exploited via a web client.	Horde Help Viewer Remote PHP Code Execution CVE-2006-1491	7.0	Security Focus, Bugtraq ID: 17292, March 29, 2006 SUSE Security Summary Report, SUSE-SR:2006:007, March 31, 2006 Gentoo Linux Security Advisory, GLSA 200604-02, April 4, 2006 **Debian Security Advisories, DSA-1033-1 & DSA-1034, April 12 & 14, 2006**
interAKTIVnet GmbH interaktiv.shop V.5, V.4	Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of the 'pn' and 'sbeg' parameters before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, Proofs of Concept exploits have been published.	Interaktiv.shop Multiple Cross-Site Scripting CVE-2006-1709	3.3	Secunia Advisory: SA19622, April 13, 2006
Internet Photoshow Internet Photoshow 1.3	A file include vulnerability has been reported in 'index.php' due to insufficient verification of the "page' parameter, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Internet Photoshow File Include	Not Available	Secunia Advisory: SA19726, April 19, 2006
Jax Scripts Jax Guestbook 3.50	A Cross-Site Scripting vulnerability has been reported in 'Jax_guestbook.PHP' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	Jax Guestbook Cross-Site Scripting	Not Available	Security Focus, Bugtraq ID: 17560, April 17, 2006
LifeType LifeType 1.0.3	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of the 'show' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	LifeType Template Cross-Site Scripting CVE-2006-1808	1.9	Secunia Advisory: SA19646, April 17, 2006
LinPHA LinPHA 1.1	Several vulnerabilities have been reported: Cross-Site Scripting vulnerabilities were reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported due to insufficient sanitization of unspecified input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.	LinPHA Cross-Site Scripting & SQL Injection CVE-2006-1848	Not Available	Secunia Advisory: SA19719, April 19, 2006

	No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.			
ModernGigabyte ModernBill 4.3-4.3.2	SQL injection vulnerabilities have been reported in 'user.php' due to insufficient sanitization of the 'id' parameter and in 'admin.php' due to insufficient sanitization of the 'where' and 'order' parameters, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit has been published.	ModernBill Multiple SQL Injection CVE-2006-1853	Not Available	Secunia Advisory: SA19641, April 19, 2006
MODxCMS MODxCMS 0.9.1	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'index.php' due to insufficient sanitization of the 'id' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a Directory Traversal vulnerability was reported in 'index.php' due to insufficient sanitization of the 'id' parameter, which could let a remote malicious user obtain sensitive information. Patch available Vulnerabilities can be exploited through a web client; however, Proof of Concept exploits have been published.	MODx Cross-Site Scripting & Directory Traversal CVE-2006-1820 CVE-2006-1821	4.7 (CVE-2006-1820) 4.7 (CVE-2006-1821)	Security Tracker Alert ID: 1015940, April 15, 2006
Mozilla. org Mozilla Browser prior to 1.7.13, Seamonkey prior to 1.0.1, Thunderbird prior to 1.0.8, 1.5 - 1.5.0.1, Firefox, 1.5 - 1.5.0.1	A vulnerability has been reported in the 'Print Preview' feature, which could let a remote malicious user obtain chrome privileges. Updates available Fedora RHSA-2006-0328.html RHSA-2006-0329.html Currently we are not aware of any exploits for this vulnerability.	Mozilla 'Print Preview' Arbitrary Code Execution CVE-2006-1727	7.0	Security Tracker Alert IDs, 1015926, 1015927, 1015928, 1015929, April 14, 2006 RedHat Security Advisory, RHSA-2006-0328 & 0329, April 14 & 18, 2006
Mozilla. org Mozilla Browser prior to 1.7.13, Seamonkey prior to 1.0.1, Thunderbird prior to 1.0.8, 1.5 - 1.5.0.1, Firefox, 1.5 - 1.5.0.1	A vulnerability has been reported in the 'crypto.generateCRMFRequest' method, which could let a remote malicious user execute arbitrary code. Updates available Fedora RHSA-2006-0328.html RHSA-2006-0329.html Currently we are not aware of any exploits for this vulnerability.	Mozilla Browser Suite 'crypto.generate CRMFRequest' Arbitrary Code Execution CVE-2006-1728	7.0	Security Tracker Alert IDs: 1015922, 1015923, 1015924, 015925, April 14, 2006 RedHat Security Advisories, RHSA-2006-0328 & 0329, April 14 & 18, 2006 Technical Cyber Security Alert TA06-107A US-CERT VU#932734
Mozilla. org Seamonkey 1.5 - 1.5.0.1, Thunderbird 1.5 - 1.5.0.1, Firefox 1.5 - 1.5.0.1	A vulnerability has been reported in the 'js_ValueToFunctionObject()' function, which could let a remote malicious user execute arbitrary code. Updates available Currently we are not aware of any exploits for this vulnerability.	Mozilla Security Check Arbitrary Code Execution CVE-2006-1726	7.0	Security Tracker Alert IDs: 1015931, 1015932, 1015933, April 14, 2006 Technical Cyber Security Alert TA06-107A US-CERT VU#968814
Mozilla.oeg Thunderbird prior to 1.0.8, 1.5 - 1.5.0.1; Seamonkey prior to 1.0.1; Mozilla browser prior to 1.7.13; Firefox prior to 1.0.8, 1.5 - 1.5.0.1	A integer overflow vulnerability has been reported because a remote malicious user can create an HTML based email that contains a specially crafted CSS letter-spacing property value, which could lead to the execution of arbitrary code. Updates available RHSA-2006-0328.html RHSA-2006-0329.html Currently we are not aware of any exploits for this	Mozilla Integer Overflow CVE-2006-1730	7.0	Security Tracker Alert IDs: 1015915, 1015916, 1015917, 1015918, April 14, 2005 RedHat Security Advisories, RHSA-2006-0328 & 0329, April 14 & 18, 2006

	vulnerability.			Technical Cyber Security Alert TA06-107A US-CERT VU#179014
Mozilla.org Firefox .5 - 1.5.0.1, Thunderbird 1.5 - .5.0.1, Seamonkey prior to 1.0.1	Multiple vulnerabilities have been reported because specially crafted HTML that generates DHTML can cause a memory corruption error, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. Updates available Fedora RHSA-2006-0328.html A Proof of Concept exploit has been published.	Mozilla DHTML Memory Corruption CVE-2006-1724 CVE-2006-1529 CVE-2006-1530 CVE-2006-1531 CVE-2006-1723	7.0 (CVE-2006-1724) 7.0 (CVE-2006-1529) 7.0 (CVE-2006-1530) 7.0 (CVE-2006-1531) 7.0 (CVE-2006-1723)	Security Tracker Alert IDs: 1015919, 1015920, 1015921, April 14, 2006 RedHat Security Advisory, RHSA-2006-0328, April 14, 2006 Technical Cyber Security Alert TA06-107A US-CERT VU#350262
Multiple Vendors Plone 2.1.2, 2.0.5, 2.0.4, 2.5-beta1; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	A vulnerability has been reported in 'changeMemberPortrait' and 'deletePersonalPortrait' due to a failure to properly enforce privileges, which could let a remote malicious user manipulate certain information. Hotfix available dsa-1032 Vulnerability can be exploited with standard web client applications; however a Proof of Concept exploit has been published.	Plone MembershipTool Access Control Bypass CVE-2006-1711	2.3	Security Focus, Bugtraq ID: 17484, April 12, 2006 Debian Security Advisory, DSA-1032-1, April 12,2006
Multiple Vendors PostNuke Development Team PostNuke 0.761; moodle 1.5.3; Mantis 1.0.0RC4, 0.19.4; Cacti 0.8.6 g; ADOdb 4.68, 4.66; AgileBill 1.4.92 & prior	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in the 'server.php' test script, which could let a remote malicious user execute arbitrary SQL code and PHP script code; and a vulnerability was reported in the 'tests/tmssql.php' text script, which could let a remote malicious user call an arbitrary PHP function. Adodb Cacti Moodle PostNuke AgileBill Mantis dsa-1029 dsa-1030 dsa-1031 **Gentoo** There is no exploit code required; however, a Proof of Concept exploit has been published.	ADOdb Insecure Test Scripts CVE-2006-0146 CVE-2006-0147	7.0 (CVE-2006-0146) 7.0 (CVE-2006-1047)	Secunia Advisory: SA17418, January 9, 2006 Security Focus, Bugtraq ID: 16187, February 7, 2006 Security Focus, Bugtraq ID: 16187, February 9, 2006 Debian Security Advisory, DSA-1029, April 8, 2006 Debian Security Advisory, DSA-1030-1, April 8, 2006 Debian Security Advisory, DSA-1031-1, April 8, 2006 **Gentoo Linux Security Advisory, GLSA 200604-07, April 14, 2006**

Multiple Vendors Slackware Linux 10.2, -current; RedHat Fedora Core5, Core4, Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0; Netscape 7.2, Netscape Browser 8.0.4; Mozilla Thunderbird 1.5.1, 1.5 Beta 2, 1.5, 1.0-1.0.7, 0.9, 0.8, 0.7-0.7.3, 0.6; Mozilla SeaMonkey 1.0 dev, 1.0; Mozilla Firefox 1.5.1, 1.5 beta 1 & beta2, 1.5, 1.0-1.0.7, 0.10.1, 0.10, 0.9- 0.9.3, 0.8, Firefox Preview Release; Mozilla Browser 1.8 Alpha 1 - Alpha 4, Mozilla Browser 1.8 Alpha 3 Mozilla Browser 1.8 Alpha 2 Mozilla Browser 1.8 Alpha 1 Mozilla Browser 1.7-1.7.12, 1.6, 1.5.1, 1.5, 1.4.4, 1.4.2, 1.4.1, 1.4 b, 1.4 a, 1.4 , 1.3.1, 1.3, 1.2.1, 1.2 Alpha & Beta, 1.2, 1.1 Alpha & Beta, 1.1, 1.0-1.0.2, 0.9.48, 0.9.35, 0.9.9, 0.9.2-0.9.8, M16, M15	Multiple vulnerabilities have been reported which could lead to the execution of arbitrary code, cause a Denial or Service, elevated privileges, execution of arbitrary JavaScript code, disclosure of sensitive information, bypass security restrictions, or spoofing of windows contents. New versions of the Mozilla Suite, Firefox, SeaMonkey, and Thunderbird are available to address these issues. Fedora RHSA-2006-0328.html RHSA-2006-0329.html Some of these vulnerabilities do not require exploit code.	Mozilla Suite, Firefox, SeaMonkey, & Thunderbird Multiple Remote Vulnerabilities CVE-2006-1729 CVE-2006-1045 CVE-2006-0748 CVE-2006-1725 CVE-2006-1731 CVE-2006-0749 CVE-2006-1732 CVE-2006-1733 CVE-2006-1734 CVE-2006-1735 CVE-2006-1736 CVE-2006-1737 CVE-2006-1738 CVE-2006-1739 CVE-2006-1740 CVE-2006-1741 CVE-2006-1742 CVE-2006-1790	2.3 (CVE-2006-1729) 1.9 (CVE-2006-1045) 7.0 (CVE-2006-0748) 7.0 (CVE-2006-0749) 1.9 (CVE-2006-1725) 1.9 (CVE-2006-1731) 2.3 (CVE-2006-1732) 7.0 (CVE-2006-1733) 7.0 (CVE-2006-1734) 7.0 (CVE-2006-1735) 1.9 (CVE-2006-1736) 7.0 (CVE-2006-1737) 2.3 (CVE-2006-1738) 7.0 (CVE-2006-1739) 1.9 (CVE-2006-1740) 2.3 (CVE-2006-1741) 2.3 (CVE-2006-1742) 7.0 (CVE-2006-1790)	Security Focus, Bugtraq ID: 17516, April 18, 2006 RedHat Security Advisories, RHSA-2006-0328 & 0329, April 14 & 18, 2006 Technical Cyber Security Alert TA06-107A US-CERT VU#935556 US-CERT VU#492382 US-CERT VU#736934 US-CERT VU#813230 US-CERT VU#842094 US-CERT VU#488774
MusicBox MusicBox 2.3.3 & prior	Several vulnerabilities have been reported: a script insertion vulnerability was reported in 'index.php' due to insufficient sanitization of the 'term' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported in 'index.php' due to insufficient sanitization of the 'start' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, Proof of Concept exploits have been published.	Musicbox Script Insertion & SQL Injection CVE-2006-1806 CVE-2006-1807	1.9 (CVE-2006-1806) 7.0 (CVE-2006-1807)	Secunia Advisory: SA19672, April 17, 2006
MyBB Group MyBulletinBoard 1.1	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported when handling content dispositions for HTML attachments, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported due to insufficient protection from direct access in the 'global.php' and 'inc/init.php' scripts, which could let a remote malicious user manipulate arbitrary script variables and execute arbitrary HTML and script code. Update available Vulnerabilities can be exploited through a web client; however, Proof of Concept exploits have been published.	MyBB Cross-Site Scripting & Variable Manipulation	Not Available	Secunia Advisory: SA19668, April 18, 2006
MyBB Group MyBulletinBoard 1.10	A Cross-Site Scripting vulnerability has been reported in 'Member.PHP' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code.	MyBB 'Member.PHP' Cross-Site Scripting	1.4	Security Focus, Bugtraq ID: 17492, April 13, 2006

	No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	CVE-2006-1281		
myWebland myEvent 1.2	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'addevent.php' due to insufficient sanitization of the 'event_desc' parameter before using, which could let a remote malicious user execute arbitrary HTML and script code; an SQL injection vulnerability was reported in 'addevent.php' and 'del.php' due to insufficient sanitization of the 'event_id' parameter and in 'addevent.php' due to insufficient sanitization of 'event_desc' before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported in 'myevent.php' and 'initialize.php' due to insufficient verification of the 'myevent_path' parameter before using to include files, which could let a remote malicious user execute arbitrary PHP code; and a vulnerability was reported in 'event.php' and 'viewevent.php' due to insufficient verification of the 'myevent_path' parameter before using to include files, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, Proof of Concept exploits have been published.	myEvent Multiple Remote Vulnerabilities	Not Available	Secunia Advisory: SA19680, April 18, 2006
Neuron Blog Neuron Blog 1.1	Multiple HTML injection & SQL injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input before using in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	Neuron Blog Multiple HTML Injection & SQL Injection	Not Available	Security Focus, Bugtraq ID: 17552, April 17, 2006
nfec.de Rechnungs Zentrale V2 1.1.3	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'mod/authent.php4' due to insufficient sanitization of the 'user' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a file include vulnerability was reported in 'mod/authent.php4' due to insufficient verification of the 'rootpath' parameter, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, Proof of Concept exploits have been published.	Rechnungs Zentrale V2 SQL Injection & File Include	Not Available	Secunia Advisory: SA19728, April 19, 2006
Novell GroupWise Messenger prior to 2.0 Public Beta 2	A buffer overflow vulnerability has been reported in the 'Accept-Language:' header due to a boundary error, which could let a remote malicious user execute arbitrary code. Update information An exploit script, novell_messenger_acceptlang.pm, has been published.	Novell GroupWise Messenger Remote Buffer Overflow CVE-2006-0992	10.0	Novell Technical Information Document, TID10100861, April 13, 2006
Opera Software Opera Web Browser 8.52 & prior	A buffer overflow vulnerability has been reported due to insufficient bounds checking of user-supplied input before using in a string-copy operation, which could let a remote malicious user cause a Denial of Service. Updates available A Proof of Concept exploit has been published.	Opera Web Browser Stylesheet Attribute Buffer Overflow CVE-2006-1834	Not Available	SEC-CONSULT Security Advisory 20060413-0, April 13, 2006
Oracle JD Edwards EnterpriseOne 8.x, OneWorld 8.x, Oracle Application Server 10g, Collaboration Suite 10.x, Database 10g, 8.x, E-Business Suite 11i, Enterprise Manager 10.x, PeopleSoft Enterprise Tools	Oracle has released a Critical Patch Update advisory for April 2006 to address multiple vulnerabilities. Some have an unknown impact, and others can be exploited to conduct SQL injection attacks. Patch information Currently we are not aware of any exploits for these vulnerabilities.	Oracle Products Multiple Vulnerabilities	Not Available	Oracle Security Advisory, April 18, 2006 Technical Cyber Security Alert TA06-109A US-CERT VU#241481 US-CERT VU#240249

8.x, Pharmaceutical Applications 4.x, Workflow 11.x, Oracle9i Application Server, Oracle9i Collaboration Suite, Oracle9i Database Enterprise Edition, Standard Edition, Oracle9i Developer Suite				
PAJAX PAJAX 0.5.1 & prior	Several vulnerabilities have been reported: a vulnerability was reported in 'pajax_call_ dispatcher.php' due to insufficient sanitization of the 'method' and 'args' parameters before using, which could let a remote malicious user execute arbitrary PHP code; and a vulnerability was reported due to insufficient sanitization of the 'className' variable before using to include files, which could let a remote malicious user execute arbitrary PHP code. Updates available There is no exploit code required; however, a Proof of Concept exploit script, pajax-0.5.1.txt, has been published.	PAJAX Multiple Arbitrary PHP Code Execution CVE-2006-1551 CVE-2006-1789	7.0 (CVE-2006-1551) 2.3 (CVE-2006-1789)	Secunia Advisory: SA19653, April 14, 2006
Papoo Papoo 2.1.5, 2.1.2	A Cross-Site Scripting vulnerability has been reported in several scripts due to insufficient filtering of HTML code from user-supplied input in the 'menuid,' 'forumid,' and 'reporeid_print' parameters before displaying the input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit script, Papoo-2.1.5, has been published.	Papoo Cross-Site Scripting	Not Available	Security Tracker Alert ID: 1015939, April 15, 2006
Patronet CMS Patronet CMS 0	A Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	PatroNet CMS Cross-Site Scripting CVE-2006-1783	2.3	Security Focus, Bugtraq ID: 17495, April 11, 2006
PHP121 PHP121 1.4	An SQL injection vulnerability has been reported in 'php121login.php' due to insufficient sanitization before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, Proof of Concept exploit scripts, PHP121_poc and php121im_14_sql_xpl, have been published.	PHP121 SQL Injection CVE-2006-1828	5.6	Security Tracker Alert ID: 1015936, April 14, 2006
phpAlbum.net phpalbum 0.3.2 3, 0.2.3	A file include vulnerability has been reported in 'Language.PHP' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script, phpalbum_poc, has been published.	PHPAlbum File Include CVE-2006-1839	Not Available	Security Focus, Bugtraq ID: 17526, April 15, 2006
phpBB Group phpBB 2.0.9	A vulnerability has been reported in 'BBCode.tpl' which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	phpBB BBCode.TPL PHP Code Execution	Not Available	Security Focus, Bugtraq ID: 17573, April 17, 2006
phpFaber TopSites 0	A Cross-Site Scripting vulnerability has been reported in 'Index.PHP' due to insufficient sanitization of the 'page' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	phpFaber TopSites Cross-Site Scripting	Not Available	Security Focus, Bugtraq ID: 17542, April 17, 2006

phpGraphy phpGraphy 0.9.12 rc1, 0.9.9 a, 0.9 .11, 0.9 .10	A vulnerability has been reported in 'index.php' due to an insecure authentication process, which could let a remote malicious user obtain unauthorized access. Updates available Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	PHPGraphy Authentication Bypass	Not Available	Secunia Advisory: SA19705, April 18, 2006
phpGuestbook phpGuestbook 0.0.2, 1.0	An HTML injection vulnerability has been reported in 'PhpGuestbook.php' due to insufficient sanitization of the 'Name,' 'Website,' and 'Comment' fields, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	PHPGuestbook HTML Injection CVE-2006-1824	Not Available	Security Focus, Bugtraq ID: 17537, April 15, 2006
phpLinks phpLinks 2.1.3 1 & prior	A Cross-Site Scripting vulnerability has been reported in 'Index.PHP' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	phpLinks Cross-Site Scripting CVE-2006-1825	7.0	Security Focus, Bugtraq ID: 17586, April 18, 2006
phpLister phpLister 0.4.1	A Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	PHPLister Cross-Site Scripting	Not Available	Security Focus, Bugtraq ID: 17591, April 18, 2006
phpWebFTP phpWebFTP 3.2	A Directory Traversal vulnerability has been reported in' Index.PHP' due to insufficient verification of the 'language' parameter, which could let a remote malicious user retrieve and execute arbitrary files. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	PHPWebFTP Directory Traversal CVE-2006-1812 CVE-2006-1813	4.7 (CVE-2006-1812) 4.7 (CVE-2006-1813)	Security Focus, Bugtraq ID: 17557, April 17, 2006
phpWebsite Development Team phpWebsite 0.10.2 & prior	A file include vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'hub_dir' parameter, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script, PHPWebSite_fi_poc, has been published.	PHPWebSite File Include CVE-2006-1819	7.0	Secunia Advisory: SA19647, April 17, 2006
PlaNet Concept planetSearch + 0	A Cross-Site Scripting vulnerability has been reported in 'planetsearchplus.php' due to insufficient sanitization of the "search_exp" parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	planetSearch+ Cross-Site Scripting CVE-2006-1801	2.3	Secunia Advisory: SA19681, April 17, 2006
Plexum Plexum X5	An SQL injection vulnerability has been reported in 'plexum.php' due to insufficient sanitization of the 'pagesize' and 'startpos' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Plexum X5 SQL Injection	Not Available	Secunia Advisory: SA19720, April 19, 2006

PMTool PMTool 1.2.2	An SQL injection vulnerability has been due to insufficient sanitization of the 'order' parameter in multiple files included by 'index.php' before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	PMTool SQL Injection	Not Available	Security Focus, Bugtraq ID: 17599, April 19, 2006
Power Scripts.org PowerClan 1.14	An SQL injection vulnerability has been reported in 'Member.PHP' due to insufficient sanitization of the 'memberid parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	PowerClan SQL Injection CVE-2006-1805	7.0	Security Focus, Bugtraq ID: 17528, April 13, 2006
S9Y Serendipity 1.0.beta 2	A script insertion vulnerability has been reported in 'Config.PHP' due to insufficient sanitization, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited through the use of a web client.	Serendipity Blog Script Injection	Not Available	Security Focus, Bugtraq ID: 17566, April 17, 2006
scriptsfrenzy.com Article Publisher Pro 1.0.1	Several SQL injection vulnerabilities have been reported: an SQL injection vulnerability was reported in 'category.php' due to insufficient sanitization of the 'cname' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and an SQL injection vulnerability was reported in 'articles.php' due to insufficient sanitization of the 'art_id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit has been published.	Article Publisher Pro Multiple SQL Injection CVE-2006-1852	Not Available	Security Focus, Bugtraq ID: 17595, April 19, 2006
Script-solution.de Boardsolution 1.12	A Cross-Site Scripting vulnerability has been reported in 'Index.PHP' due to insufficient sanitization of the 'keyword' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	Boardsolution Cross-Site Scripting	Not Available	Security Focus, Bugtraq ID: 17549, April 17, 2006
ShoutBOOK ShoutBOOK 1.1	Several vulnerabilities have been reported: an HTML injection vulnerability was reported in 'global.php' due to insufficient sanitization of the 'NAME' and 'COMMENTS' parameters, which could let a remote malicious user execute arbitrary HTML and script code; and an HTML injection vulnerability was reported in 'global.php' due to insufficient sanitization of the 'LOCATION' and 'URL' parameters, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited via a web client.	ShoutBOOK Multiple HTML Injection CVE-2006-1842 CVE-2006-1843	Not Available	Secunia Advisory: SA19704, April 18, 2006
SibSoft Ltd. CommuniMail 1.2	Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of the 'list_id' parameter in 'mailadmin.cgi' and in 'templates.cgi' due to insufficient sanitization of the 'form_id' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit has been published.	CommuniMail Multiple Cross-Site Scripting	Not Available	Security Focus, Bugtraq ID: 17602, April 19, 2006

SimpleMedia SimpleBBS 1.0.6-1.1	Several vulnerabilities have been reported: a vulnerability was reported due to insufficient sanitization of the 'name' parameter when adding a new topic, which could let a remote malicious user execute arbitrary PHP code; and a vulnerability was reported in 'data/posts.php' due to insufficient verification of the 'language' cookie parameter before using to include files, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script, SimpleBBS-RCE-posts.php.pl, has been published.	SimpleBBS Remote Arbitrary Command Execution CVE-2006-1800	7.0	Security Focus, Bugtraq ID: 17501, April 13, 2006
Simplog Simplog 0.9.2 & prior	Multiple vulnerabilities have been reported: a file include vulnerability was reported in 'doc/index.php' due to insufficient sanitization of the 's' parameter, which could let a remote malicious user execute arbitrary PHP code; an SQL injection vulnerability was reported in 'index.php' due to insufficient sanitization of the 'blogid' parameter and in 'archive.php' due to insufficient sanitization of the 'blogid,' 'm,' and 'y' parameters, which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported in 'adodb/server.php' and 'adodb/texts/tmssql.php' due to insecure test scripts, which could let a remote malicious user execute arbitrary SQL code or call an arbitrary PHP function; and a Cross-Site scripting vulnerability was reported in 'login.php' due to insufficient sanitization of the 'btag' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. Update to version 0.9.3. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit script, simplog-0.9.2-remote-command-execution.php, has been published.	Simplog Multiple Vulnerabilities CVE-2006-1776 CVE-2006-1777 CVE-2006-1778 CVE-2006-1779	7.0 (CVE-2006-1776) 7.0 (CVE-2006-1777) 7.0 (CVE-2006-1778) 7.0 (CVE-2006-1779)	Secunia Advisory: SA19628, April 12, 2006
Snipe Gallery Snipe Gallery 3.1.4 & prior	Multiple Cross-Site Scripting vulnerabilities have been reported in 'view.php,' 'search.php,' and 'image.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, Proof of Concept exploits have been published.	Snipe Gallery Multiple Cross-Site Scripting CVE-2006-1826	7.0	Security Focus, Bugtraq ID: 17543, April 17, 2006
Sphider Sphider 1.3 & prior	A vulnerability has been reported in 'admin/configset.php' due to insufficient verification of the 'settings_dir' parameter before using to include files, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, exploit scripts, sphider_poc.pl and sphider_13_xpl_pl, have been reported.	Sphider File Include CVE-2006-1784	7.0	Secunia Advisory: SA19642, April 13, 2006
Sysinfo Sysinfo 1.21	Several vulnerabilities have been reported: a vulnerability was reported in 'sysinfo.cgi' due to insufficient sanitization of the 'name' parameter before using, which could let a remote malicious user execute arbitrary shell commands; and a vulnerability was reported because it is possible to obtain the full path to the installation when the 'action' parameter is set to 'debugging.' Update available Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit script, sysinfo_poc, has been published.	Sysinfo Input Validation CVE-2006-1831 CVE-2006-1832	Not Available	Secunia Advisory: SA19690, April 17, 2006
The War Forge Warforge.NEWS 1.0	Multiple input validation vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML, script code, and SQL code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client.	Warforge.NEWS Multiple Input Validation CVE-2006-1817 CVE-2006-1818	1.9 (CVE-2006-1817) 1.9 (CVE-2006-1818)	Security Focus, Bugtraq ID: 17520, April 14, 2006

Thwboard Thwboard Beta 2.8-2.84	An SQL injection vulnerability has been reported in 'Showtopic.PHP' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	ThWboard SQL Injection	Not Available	Security Focus, Bugtraq ID: 17606, April 19, 2006
Tiny Web Gallery Tiny Web Gallery 1.4	A Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'twg_album' parameter before returning to users, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	Tiny Web Gallery Cross-Site Scripting CVE-2006-1802	2.3	Security Focus, Bugtraq ID: 17536, April 15, 2006
TinyPHP Forum TinyPHPForum 3.6	Multiple Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client.	TinyPHPForum Multiple Cross-Site Scripting	Not Available	Security Focus, Bugtraq ID: 17553, April 17, 2006
TotalCalendar TotalCalendar 2.x	A file include vulnerability has been reported due to insufficient verification of the 'inc_dir' parameter in 'about.php' and 'auth.php' before using to include files, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	TotalCalendar File Include	Not Available	Secunia Advisory: SA19730, April 19, 2006

[back to top]

Wireless Trends & Vulnerabilities

This section contains wireless vulnerabilities, articles, and malicious code that has been identified during the current reporting period.

- Cisco Wireless Lan Solution Engine Cross-Site Scripting & Privilege Elevation: Two vulnerabilities have been reported in exist in the CiscoWorks Wireless LAN Solution Engine (WLSE). One is a Cross-Site Scripting vulnerability and the other one is a privilege elevation vulnerability.
- Mobile Browsing Seen Changing Face Of The Web: The rapid pace of mobile phone installation and the development of wireless networks are driving robust growth in the use of phones for browsing. People are turning to mobile phones for Internet use more quickly than they're adopting laptops for the same purpose in many parts of the world.
- Rivals Agree on 802.11s Wireless Mesh Proposal: An agreement was made in March on a joint IEEE mesh networking standard. The Intel-and Firetide-led SEE Mesh, which had put forward a proposal to compete with Nortel's Wi-Mesh Alliance, resolved their differences and moved forward with a joint proposal that should be voted in as the draft standard for 802.11s, the IEEE mesh networking standard.

[back to top]

General Trends

This section contains brief summaries and links to articles which discuss or present information pertinent to the cyber security community.

- McAfee Warns About Increasing Prevalence of Rootkits: According to a McAfee research study, the use of stealth technologies that conceal both malware and commercially viable Potentially Unwanted Programs (PUPs) is on the rise. In the last three years, the incident rate of stealth technology has increased by more than 600 percent. McAfee considers malicious programs using stealth technology to be rootkits, distinct from commercial applications that use stealth technology.
- Spam Attack Keeps Bagle Boiling: According to researchers at F-Secure, a new attack aimed at computers infected with the Bagle virus threatens to generate scads of spam e-mail campaigns. The attacked, 'SpamTool.Win32.Bagle.g' involves a new set of URLs being sent to machines infected with Bagle.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script),

trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folder.
2	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
3	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
4	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
5	Mytob-GH	Win32 Worm	Stable	November 2005	A variant of the mass-mailing worm that disables security related programs and allows other to access the infected system. This version sends itself to email addresses harvested from the system, forging the sender’s address.
6	Nyxum-D	Win32 Worm	Stable	March 2006	A mass-mailing worm that turns off anti-virus, deletes files, downloads code from the internet, and installs in the registry. This version also harvests emails addresses from the infected machine and uses its own emailing engine to forge the senders address.
7	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
8	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
9	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
10	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.

Table updated April 19, 2006

[back to top]

Last updated April 20, 2006